

## UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of  
 (Briefly describe the property to be searched  
 or identify the person by name and address)      )  
 Information related to the Kik Messenger dadof2boys74      )  
 )      Case No. 1:19-mj-385

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Information related to the Kik Messenger account dadof2boys74, stored at premises owned, maintained, controlled or operated by stored at any premises owned, maintained, controlled, or operated by MediaLab.AI, Inc. See Attachment A

located in the Central District of California, there is now concealed (identify the person or describe the property to be seized):

Evidence of, instrumentalities used in committing, and fruits of the crimes of 18 U.S.C. Sections 2252A(a)(2)(A) and 2252A(a)(5)(B) as further described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

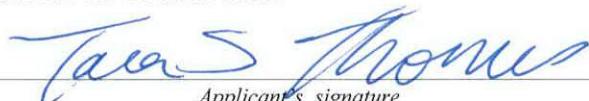
- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2252A(a)(2)(A)	Receipt/Distribution of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

- Continued on the attached sheet.
- Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
 Applicant's signature

Tara S. Thomas, FBI Special Agent  
 Printed name and title

Sworn to before me and signed in my presence.

Date: 12/11/19

City and state: Greensboro, North Carolina

  
 Judge's signature

L. Patrick Auld, U.S. Magistrate Judge  
 Printed name and title

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to records and other information related to the Kik Messenger account dadof2boys74, which is stored at any premises owned, maintained, controlled, or operated by MediaLab.AI, Inc., a company headquartered in the Central District of California.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be Disclosed by MediaLab.AI.**

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab.AI, Inc., including any information that has been deleted but is still available to MediaLab.AI, Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), MediaLab.AI, Inc., is required to disclose the following information to the government for each account listed in Attachment A:

- a. All information concerning messages sent or received by the account, including but not limited to, transactional chat logs, chat platform logs, files sent or received, and substance if available;
- b. Logs of users blocked by the account or the users who have blocked the account;
- c. Abuse reports from or concerning the account;
- d. Kik Groups that the account belongs to;
- e. IP address logs, including registration IP;
- f. Location information;
- g. All business records and subscriber information, in any form kept, pertaining to the individual account, including subscribers' registration details, full names, addresses, ESN (Electronic Serial Number) or other

unique identifier for the device(s) associated with the account, date of birth, telephone numbers, password records, and other identifiers or records associated with the account; and

h. Any and all communications between MediaLab.AI, Inc. (i.e. Kik Messenger administration) and the account.

**The Provider is hereby ordered to disclose the above information to the government within FOURTEEN DAYS of service of this warrant.**

## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 2252A(a)(5)(B) and (a)(2)(A) by the user(s) of the account identified on Attachment A, in the form of the following:

- a) records and information constituting child pornography, as defined in 18 U.S.C. 2256(8);
- b) records and information constituting child erotica;
- c) records and information revealing access to and/or trafficking of child pornography and identity of those participating, to include information about specific transactions and instances of access.

- d) records and information revealing the sexual exploitation of or sexual interest in any minor;
- e) records and information constituting or revealing the identity and age of any minor victim;
- f) transactional and location information pertaining to any items authorized to be seized under this section (Section II), including log files revealing information such as time, date, and IP address used;
- g) records and information constituting or revealing participation in groups or communication with others that provide or make accessible child pornography; and
- h) Records revealing or indicating who created and accessed the Kik account identified in Attachment A, including records revealing subscriber information, IP addresses, mobile devices used, and images depicting individuals who may be the user and/or his/her associates.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data).

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Tara S. Thomas, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I am investigating offenses related to child sexual exploitation. I make this affidavit in support of an application for a warrant to search information related to Kik Messenger account dadof2boys74 ("SUBJECT ACCOUNT"). The information is stored at premises owned, maintained, controlled, or operated by MediaLab.AI, Inc., a company headquartered in the Central District of California. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MediaLab.AI, Inc. to disclose to the government records and other information in its possession, pertaining to the SUBJECT ACCOUNT.

2. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe

are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES.

**AFFIANT BACKGROUND**

3. I am a Special Agent of the Federal Bureau of Investigation (“FBI”), and have been since March of 2008. My initial training consisted of a twenty-week FBI new agent course during which I received instruction on various aspects of federal investigations, ranging from economic espionage and child pornography, to kidnapping and computer intrusions. In addition, I have received more than 350 hours of training related to computers and cyber matters, to include investigations of cybercrime. I am currently assigned to the Charlotte Division and stationed at the Greensboro Resident Agency. Prior to joining the FBI, I worked in law enforcement for over eight years as a police officer and sheriff's investigator. I have been the case agent or supporting agent in numerous investigations, including investigations involving the production, distribution, and possession of child pornography. I have received training in the area of child pornography and child exploitation, and have observed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in

all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2252A, and I am authorized by law to request a search warrant. As a Special Agent, I am authorized to investigate violations of laws and to execute warrants issued under the authority of the United States.

4. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

#### **STATUTORY AUTHORITY**

5. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

#### DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating

in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

f. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

g. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the

structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

i. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

j. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

k. "Remote computing service", as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

l. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons

of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

m. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

#### BACKGROUND ON KIK MESSENGER

7. Kik Messenger (hereinafter "Kik") is a mobile application designed for chatting or messaging owned and operated by MediaLab.AI, Inc., a United States based holding company of Internet brands. Kik was formerly owned by Kik Interactive, Inc., a Canadian based company. MediaLab.AI, Inc., acquired the Kik application in October 2019.

8. According to "Kik's Guide for Law Enforcement," published in July 2019, to use the Kik application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an

account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

9. According to "Kik's Guide for Law Enforcement," Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

10. According to "Kik's Guide for Law Enforcement," the information that Kik may be able to provide to law enforcement pursuant to a search warrant includes the following:

*Basic Subscriber Data:* Current first and last name and email address, Link to the most current profile picture or background photo, Device related information, Account creation date and Kik version, Birthdate and email address used to register the account.

### *Historical IP Addresses*

*Transactional Chat Log:* Log of all the messages that a user has sent and received, including sender username, receiver username(s), timestamps, IP of the sender and word count. (does not include the actual message that was sent)

*Chat Platform Log:* Log of all the media files that a user has sent and received, including sender username, receiver username(s), timestamps, IP of the sender, media type, and content ID.

*Photographs and/or Videos:* Media files sent or received by the user for last 30 days.

*Roster Log:* Log of usernames added and blocked by the subject user, including timestamps.

*Abuse Reports:* Transcript of reported chat history against the subject user, including sender username, receiver username, timestamps, actual message, and content IDs.

*Email Events:* Log of all the emails that have been associated with a username

*Registration IP:* IP address associated to the username when the account was registered, including timestamp.

### **PROBABLE CAUSE**

11. On December 5, 2019, an FBI undercover agent, known as an “Online Covert Employee” (OCE) interacted with Kik user “dadof2boys74” in a group chat and a private message chat.

12. On December 5, 2019, Kik user "dadof2boys74" entered the Kik chat group #boy11nk with a display name of "Send link upon entry". The OCE, who acts as an administrator of the room, noticed "dadof2boys74" enter the room and reminded him to read the rules. At 6:50 p.m., "dadof2boys74" posted a MEGA cloud storage account hyperlink to the group chat followed by the word "ping". MEGA is a cloud storage service similar to Dropbox. Based on my training and experience, I know that MEGA and Dropbox cloud storage platforms are often used by individuals on Kik who engage in the trafficking of child pornography. Instead of sending child pornography files via Kik, these individuals will send hyperlinks to cloud storage accounts containing child pornography via Kik.

13. The OCE clicked on the hyperlink and reviewed the content stored in the MEGA cloud storage account. The OCE noted there was approximately 1.10 gigabytes of child pornography. Some of the videos included prepubescent boys engaging in oral and anal sex with other minors and adults. The videos were in a folder called "VIDS02".

14. The OCE then began chatting with "dadof2boys74" to ascertain whether he had access to children, and if so, whether he was sexually abusing them. The OCE acknowledged "dadof2boys74" for reading the rules and asked how young his boys were. The user "dadof2boys74" said they were 10 and 6

years old. The OCE replied that he had a purported nephew with whom he was sexually active. The user "dadof2boys74" was asked his age and advised he was a 36 year old male living in the United States. He later asked the OCE if he "traded pics" of his purported nephew. The OCE replied he was into real life stuff, not child porn acquired from the internet. The user "dadof2boys74" replied, "True me too that's why I trade stuff of my boys and me but it's hard finding someone with what I want...Yeah, all my pics/vid I took myself". The OCE replied to "dadof2boys74" that he was interested and asked how recent the videos and photos were and sent a photo of a digitally altered young male to user "dadof2boys74" whom the OCE identified as his nephew Billy (not a real child).

15. The user "dadof2boys74" responded "Poor he's a hottie and mmmm". User "dadof2boys74" then sent a photograph of two minor boys standing in what appears to be the lobby/waiting area of a restaurant, identifying them as two of his children, "Anthony- the taller one and Austin- the short one". The OCE then sent a photograph to user "dadof2boys74" of a boy (not a real child) lying down with his underwear exposed. The OCE told "dadof2boys74" that Billy wasn't feeling well. The OCE and "dadof2boys74" exchanged a few more texts expressing admiration for each of the children and asking what sexual activities they like to do.

16. The user "dadof2boys74" then sent five photographs of Austin and Anthony at different locations throughout a residence at an unknown location. The first purportedly depicted Austin in his room and the next one depicted Austin in the bathtub (no genitalia could be observed in the photo). The third photo was a toddler who appeared to be urinating from a front porch. The toddler's buttocks were showing. The next photo purportedly depicted Austin in a swimming pool, and the last photo purportedly depicted Anthony eating a bowl of pasta. The user "dadof2boys74" further described the sexual activity between himself and the two boys: "Normally just sucking and jerking but I do fuck Austin when it's just me and him". "I'm 8in hard and I can get 4-5in it n Austin".

17. OCE sent a third photograph of "Billy" (not a real child) and advised "dadof2boys74" that he was "out cold". The OCE then sent a photograph of a prosthetic penis to "dadof2boys74". The user "dadof2boys74" replied, "Fuck I would pound tf out Austin with that". The OCE asked "dadof2boys74" if he had any recent videos of what he had done before and reiterated the OCE was into real life meetups. The user "dadof2boys74" then asked OCE to "take a quick pic of his cock. I would do meet ups with my boys but just getting them away from their mom long enough. She don't know about the fun 'the boys' have lol". OCE told "dadof2boys74" that he was located in

Tennessee. The user "dadof2boys74" responded that he was located in West Virginia.

18. The user "dadof2boys74" went on to explain that he preferred "newborn and 5-11". He told the OCE he was trying to get his wife pregnant so he could have another toy. the OCE asked "dadof2boys74" how he kept the boys from telling their mother or another adult about the sexual encounters. The user "dadof2boys74" replied, "Because it's a big boy Secret and only us 3 can ever know about". As the chats progressed, "dadof2boys74" stated he has sex with the boys, "probably 3-4 times a week sometimes twice a day".

19. The OCE asked "dadof2boys74" where he kept the videos he produced. The user "dadof2boys74" told the OCE that he keeps them in a Dropbox account that he installs and un-installs on his phone and that only he knows the password and user to it. Purportedly anticipating another child with his wife, "dadof2boys74" told the OCE he was looking forward to having a baby boy so he could suck and jerk the tiny cocks and try not to get caught in the public bathroom. OCE asked when the last time "dadof2boys74" was sexually active with one of his boys, to which he replied, "Monday" meaning December 2, 2019.

20. On December 6, 2019, an emergency disclosure request was sent to Kik. Kik provided subscriber information for user "dadof2boys74" that included the following:

First name:	All
Last Name:	Love
Email:	kahdhrbydhe697@yahoo.com (unconfirmed) <sup>1</sup>
Registration	Timestamp: 12/05/2019 at 12:28 p.m.
Device:	iPhone

21. Kik IP address records logged user "dadof2boys74" using the IP address 71.73.234.41 four times on December 5, 2019 between 6:29 p.m. and 6:59 p.m. A query of the American Registry for Internet Numbers ("ARIN") online database revealed IP address 71.73.234.41 as being registered to Charter Communications Inc.

22. On December 10, 2019, an administrative summons was issued to Charter Communications, Inc. for account subscriber information associated with IP address 71.73.234.41. As a result of the summons, Charter Communications, Inc., provided the following account information:

Subscriber Name:	Jessie Reynolds
Subscriber Address:	800 Oaklawn Drive, Thomasville, NC 27360
Phone Number:	(336) 561-9065

---

<sup>1</sup> Yahoo has no record of this email address.

23. The Charter Communications, Inc., records indicate that IP address 71.73.234.41 was assigned to the account of Jessie Reynolds from January 23, 2019, to December 10, 2019.

24. On December 10, 2019, I reviewed the MEGA hyperlink provided by "dadof2boys74" which contained 60 videos. The following is a description of three of the videos:

- a. "man fucks 12yo two ways.avi" depicts an adult male anally raping a prepubescent minor male approximately 12 years of age. The video is 6 minutes and 54 seconds long.
- b. "\_2\_boys\_in\_a\_bath\_10yo\_sucks\_13yo\_till\_he\_cums\_in\_mouth\_2.24\_2\_.mpeg4.mp4" depicts two prepubescent males approximately 13 years of age and 10 years of age naked in a bath tub. The older boy anally penetrates the younger boy, and then the younger boy provides oral stimulation to the older boy until he ejaculates. The video is 2 minutes and 24 seconds long.
- c. "Webcam 11yo boy (beautiful cock).avi" depicts a naked prepubescent male using a webcam to communicate online and display his penis from multiple angles and at different states of erection. The video is 5 minutes and 39 seconds long.

## INFORMATION REGARDING INFORMATION TO BE SEIZED

25. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require MediaLab.AI, Inc., to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment A. Upon receipt of the information described in Section I of Attachment A, government-authorized persons will review that information to locate the items described in Section II of Attachment A.

26. Because the warrant will be served on MediaLab.AI, Inc., who will then compile the requested records at a time convenient to MediaLab.AI, Inc., reasonable cause exists to support execution of the requested warrant at any time day or night.

## CONCLUSION

27. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States ... that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the

presence of a law enforcement officer is not required for the service or execution of this warrant.



Tara S. Thomas  
Tara S. Thomas  
Special Agent  
Federal Bureau of Investigations

Sworn and subscribed before me this 11<sup>th</sup> day of December, 2019.



L. Patrick Auld  
L. Patrick Auld  
United States Magistrate Judge